SPYWOLF

Security Audit Report
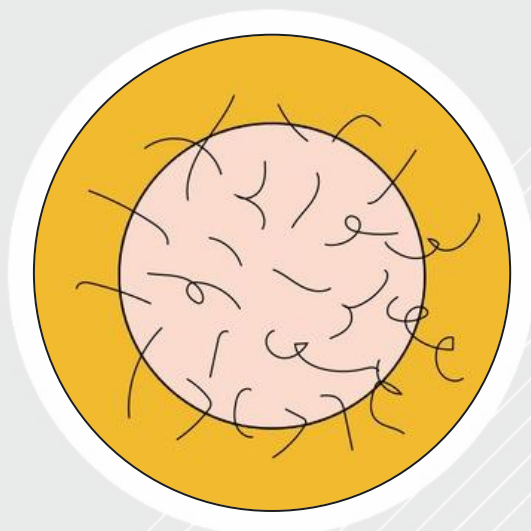
Completed on
August 3, 2023

OVERVIEW

This audit has been prepared for **BALL** to review the main aspects of the project to help investors make make an informative decision during their research process.

You will find a a summarized review of the following key points:

- ✔ Contract's source code
- ✔ Owners' wallets
- ✔ Tokenomics
- ✔ Team transparency and goals
- ✔ Website's age, code, security and UX
- ✔ Whitepaper and roadmap
- ✔ Social media & online presence

> *"The results of this audit are purely based on the team's evaluation and does not guarantee nor reflect the projects outcome and goal"*
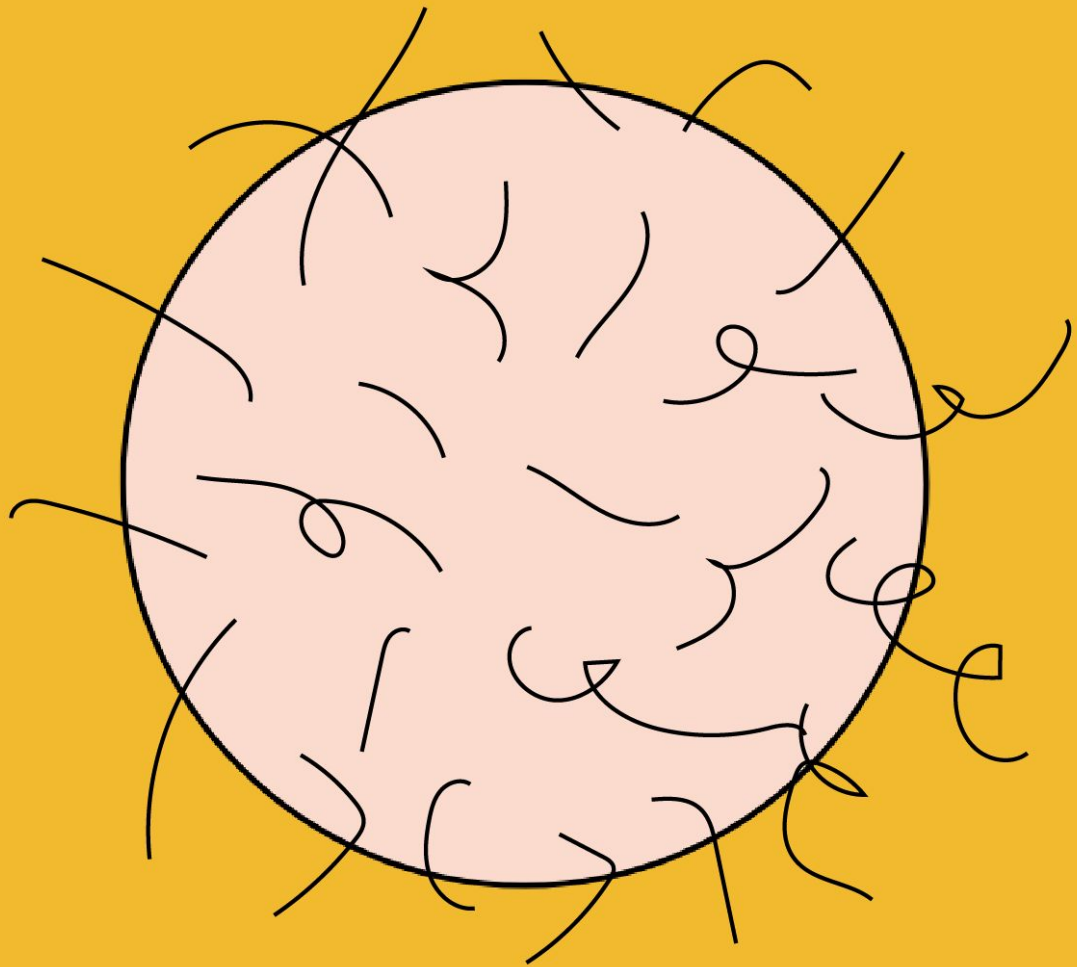>
> – SPYWOLF Team –

SPYWOLF.CO

TABLE OF CONTENTS

BALL ERC

PROJECT DESCRIPTION

According to the project's website:

"$BALL is literally unique, living alone on the blockchain. Do you have the BALLS to join the $BALL movement ?"

Release Date: Presale starts in August, 2023

Category: Meme

01

CONTRACT INFO

Token Name
BALL

Symbol
$BALL

Contract Address
0xf67F3FCE26d222D25220a820A8923cF175B6e8e4

Network
Ethereum

Language
Solidity

Deployment Date
Aug 2, 2023

Verified?
Yes

Total Supply
42,000,000,690,000,000,000

Status
Not Launched

TAXES

Buy Tax
0%

Sell Tax
0%

- Owner can set buy/sell taxes up to 25%

Our Contract Review Process

The contract review process pays special attention to the following:

- ✓ Testing the smart contracts against both common and uncommon vulnerabilities
- ✓ Assessing the codebase to ensure compliance with current best practices and industry standards.
- ✓ Ensuring contract logic meets the specifications and intentions of the client.
- ✓ Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- ✓ Thorough line-by-line manual review of the entire codebase by industry experts.

Blockchain security tools used:

- OpenZeppelin
- Mythril
- Solidity Compiler
- Hardhat

02

TOKEN TRANSFERS STATS

Transfer Count	2
Uniq Senders	2
Uniq Receivers	2
Total Amount	6300000138000010000 $BALL
Median Transfer Amount	4200000069000000000 $BALL
Average Transfer Amount	3150000069000003000 $BALL
First transfer date	2023-08-02
Last transfer date	2023-08-03
Days token transferred	2

SMART CONTRACT STATS

Calls Count	2
External calls	2
Internal calls	0
Transactions count	2
Uniq Callers	1
Days contract called	2
Last transaction time	2023-08-03 00:01:23 UTC
Created	2023-08-02 23:20:35 UTC
Create TX	0xc37128e63c18134c7fffa7f127d39c1448bccc616fbba73c1f575babb2d5496f
Creator	0x8438d85ff4e7e775380100479740ab983e4dd003

VULNERABILITY CHECK

Design Logic	Passed
Compiler warnings.	Passed
Private user data leaks	Passed
Timestamp dependence	Passed
Integer overflow and underflow	Passed
Race conditions and reentrancy. Cross-function race conditions	Passed
Possible delays in data delivery	Passed
Oracle calls	Passed
Front running	Passed
DoS with Revert	Passed
DoS with block gas limit	Passed
Methods execution permissions	Passed
Economy model	Passed
Impact of the exchange rate on the logic	Passed
Malicious Event log	Passed
Scoping and declarations	Passed
Uninitialized storage pointers	Passed
Arithmetic accuracy	Passed
Cross-function race conditions	Passed
Safe Zeppelin module	Passed
Fallback function security	Passed

04

THREAT LEVELS

When performing smart contract audits, our specialists look for known vulnerabilities as well as logical and access control issues within the code. The exploitation of these issues by malicious actors may cause serious financial damage to projects that failed to get an audit in time. We categorize these vulnerabilities by the following levels:

High Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Medium Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Low Risk

Issues on this level are minor details and warning that can remain unfixed.

Informational

Information level is to offer suggestions for improvement of efficacy or security for features with a risk free factor.

05

FOUND THREATS

⚠️ High Risk

TradinEnabled is currently false, allowing vetted addresses to potentially sell their presale tokens before opening trade for the investors.

```
function _transfer(address from, address to, uint256 amount) private {
    require(from != address(0), "ERC20: transfer from the zero address");
    require(to != address(0), "ERC20: transfer to the zero address");
    require(amount > 0, "Transfer amount must be greater than zero");
    require(
        _tOwned[from] >= amount,
        "ERC20: transfer amount exceeds balance"
    );
    //Enable Trade after sale is finilized
    require(tradingEnabled || _isExcludedFromFee[from] || _isExcludedFromFee[to], "Trading not yet enabled!");
```

- Recommendation:
  - Owner must first enable trading for any transfer

FOUND THREATS

⚠️ Medium Risk

Owner can set buy/sell fees up to 25%.
Combined buy+sell = 50%.
When fees are above 0, there will be certain amount of tokens that will be deducted from every transaction that users make.
Deducted amount will be as much as the fees % from total amount that user had bought, sold and/or transferred.

```solidity
function setBuyFee(uint256 _buyFee) external onlyOwner {
    require(_buyFee <= 25, "Buy Fee cannot be more than 25%");
    buyFee = _buyFee;
    emit Log("We have updated the buy fee to:", buyFee);
}

function setSellFee(uint256 _sellFee) external onlyOwner {
    require(_sellFee <= 25, "Sell Fee cannot be more than 25%");
    sellFee = _sellFee;
    emit Log("We have updated the sell fee to:", sellFee);
}
```

- Recommendation:
  - Considered as good tax deduction practice is buy and sell fees combined not to exceed 25%.

ℹ️ Informational

Owner can withdraw ETH from the contract.
When this function is present, in cases ETH tokens are sent into the contract by mistake or purposefully, contract's owner can retrieve them.

```solidity
// Withdraw ETH that's potentially stuck in the Contract
function recoverETHfromContract() external onlyOwner {
    uint ethBalance = address(this).balance;
    (bool succ, ) = payable(marketingWallet).call{value: ethBalance}("");
    require(succ, "Transfer failed");
    emit AuditLog(
        "We have recover the stuck eth from contract.",
        marketingWallet
    );
}
```

Owner can withdraw any tokens from the contract except the native $BALL token.
When this function is present, in cases tokens sent into the contract by mistake or purposefully, contract's owner can retrieve them.

```solidity
function recoverTokensFromContract(
    address _tokenAddress,
    uint256 _amount
) external onlyOwner {
    require(
        _tokenAddress != address(this),
        "Owner can't claim contract's balance of its own tokens"
    );
    bool succ = IERC20(_tokenAddress).transfer(marketingWallet, _amount);
    require(succ, "Transfer failed");
    emit Log("We have recovered tokens from contract:", _amount);
}
```

06-B

ℹ️ Informational

Owner can exclude address from fees.

```solidity
function excludeFromFee(address account) external onlyOwner {
    require(_isExcludedFromFee[account] != true, "The wallet is already excluded!");
    _isExcludedFromFee[account] = true;
    emit AuditLog(
        "We have excluded the following walled in fees:",
        account
    );
}
```

RECOMMENDATIONS FOR
GOOD
PRACTICES

BALL

GOOD PRACTICES FOUND

✔ The owner cannot mint new tokens after deployment

✔ The owner cannot stop or pause the contract

1	Consider fundamental tradeoffs
2	Be attentive to blockchain properties
3	Ensure careful rollouts
4	Keep contracts simple
5	Stay up to date and track development

07

*The following tokenomics are based on the project's whitepaper and/or website:

There is no information about the token distribution on the project's website/whitepaper.

TOKENOMICS

THE TEAM

⚠️ The team is annonymous

KYC INFORMATION

No KYC

We recommend the team to get a KYC in order to ensure trust and transparency within the community.

Website URL
https://ballerc.com/

Domain Registry
HOSTINGER

Domain Expiration
2024-08-02

Technical SEO Test
Passed

Security Test
Passed. SSL certificate present

Design
Nice color scheme. Needs more variety in the imagery.

Content
Content could use more explanations about what the project is about and how it will benefit the investors.

Whitepaper
Not found

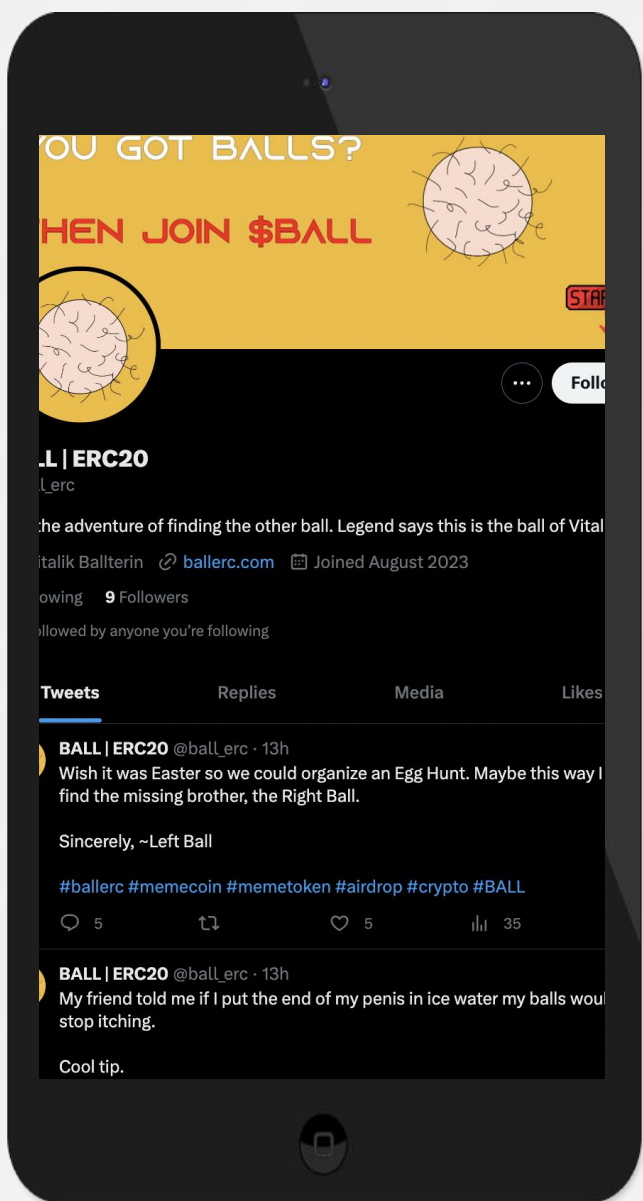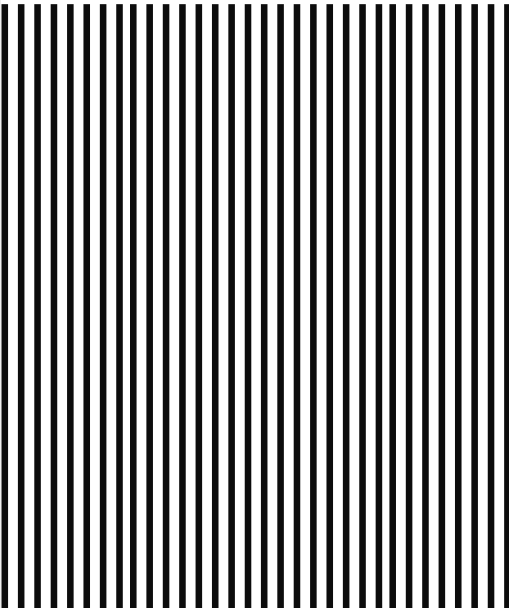## Roadmap
Yes. No specific dates

Mobile-friendly?
Yes

ONE SINGLE BALL LIVING ON THE BLOCKCHAIN.

BALL $BALL - ERC20

"Join the adventure of finding the other ball, wherever it is. Some say this is the ball of Vitalik, we will never know"

ballerc.com

SOCIAL MEDIA

& ONLINE PRESENCE

Twitter

@ball_erc

- 9 followers
- New account
- Few posts

Discord

- Not available

Telegram

@ball_erc20

- 11 members
- Active mods and devs
- New account

Medium

- Not available

11

SPYWOLF
CRYPTO SECURITY

Audits | KYCs | dApps
Contract Development

ABOUT US

We are a growing crypto security agency offering audits, KYCs and consulting services for some of the top names in the crypto industry.

- ✔ **OVER 500 SUCCESSFUL CLIENTS**

- ✔ **MORE THAN 500 SCAMS EXPOSED**

- ✔ **MILLIONS SAVED IN POTENTIAL FRAUD**

- ✔ **PARTNERSHIPS WITH TOP LAUNCHPADS, INFLUENCERS AND CRYPTO PROJECTS**

- ✔ **CONSTANTLY BUILDING TOOLS TO HELP INVESTORS DO BETTER RESEARCH**

To hire us, reach out to contact@spywolf.co or t.me/joe_SpyWolf

FIND US ONLINE

🌐 SPYWOLF.CO

✈ @SPYWOLFNETWORK

🐦 @SPYWOLFNETWORK

12

Disclaimer

This report shows findings based on our limited project analysis, following good industry practice from the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, overall social media and website presence and team transparency details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report.
While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the disclaimer below – please make sure to read it in full.

DISCLAIMER:

By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice.
No one shall have any right to rely on the report or its contents, and SpyWolf and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (SpyWolf) owe no duty of care towards you or any other person, nor does SpyWolf make any warranty or representation to any person on the accuracy or completeness of the report.
The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and SpyWolf hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, SpyWolf hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against SpyWolf, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report. The analysis of the security is purely based on the smart contracts, website, social media and team.
No applications were reviewed for security. No product code has been reviewed.